

## **A. AMENDMENTS TO SPECIFICATION**

**Please amend the specification at Page 13, lines 4-15:**

In Customization phase of ~~block~~, block 114, after a data center is created, a configuration program is used to add content information, such as Web pages or database information, to one or more servers in the data center that was created using the graphical user interface tool.

In the Customization phase, the user may save, copy, replicate, and otherwise edit and manipulate a data center design. Further, the user may apply one or more software images to servers in the data center. The selection of a software image and its application to a server may be carried out in accordance with a role that is associated with the servers. For example, if a first server has the role Web Server, then it is given a software image of an HTTP server program, a CGI script processor, Web pages, etc. If the server has the role Database Server, then it is given a software image that includes a database server program and basic data. Thus, the user has complete control over each computer that forms an element of a data center. The user is not limited to use of a pre-determined site or computer.

**Please amend the specification at Page 23, lines 13-17:**

IDC Monitor 220 also features a Monitors function 226 that allows detailed information to be collected from an IDC. Monitors function 226 may include applications monitors, server monitors, network monitors and advanced monitors, collectively identified in FIG. 2B by reference numeral 228. These monitors are described in more detail hereinafter.

Additionally, alerts may be generated if the certain thresholds are exceeded (such as network response time or disk space utilization being outside acceptable bounds). Each new IDC is

automatically constructed with a default set of monitors. Once operational, the user may tune and modify the monitoring as required.

**Please amend the specification at Page 24, line 30, through Page 25, line 2:**

Server Management function 232 of IDC Monitor 220 provides server management operations, such as login, log file access and attended scaling, referred to collectively in FIG. 2B by reference numeral 234. For example, Server Management function 232 enables interactive login to a server of an IDC using Secure Shell (ssh) or pcAnywhere); customization and addition of content to a server; and cloning of servers.

**Please amend the specification at Page 25, lines 5-8:**

Backup function 238 enables a user to modify a backup policy for an element of an IDC, carry out a data restoration operation, and view various system logs. These functions are identified collectively in FIG. 2B by reference numeral 240. Backup function 238 accesses IDC Component database 129, Customer information database 131, FML Repository 131, and Control Plane Database 135.

**Please amend the specification at Page 25, line 9-11:**

FIG. 2C is a block diagram showing pages and related functions that may be accessed through administration page 210. Available functions include Account Management function 252, Farm Management function 254, and Physical Inventory function 258. Physical Inventory 258 includes Storage 258a, Firewalls 258b, CPU 258c, Load Balancing 258d, Switches 258e and Other 258f.

**Please amend the specification at Page 25, lines 24-26:**

Physical Inventory Management ~~function 256~~ function 258 provides one or more back-end operations relating to server farm hardware, e.g., failure monitoring, fault diagnosis, processing maintenance requests, adding more elements, etc.

**Please amend the specification at Page 40, lines 11-16:**

In one specific embodiment, the boot volume (Disk 0) of a machine has a pre-defined, fixed size and can only have images that are that size installed on it. For example, the fixed size may be 8 Gb, 9 Gb, etc. Additional disks can be added and removed when the Tier is in the design or active ~~states~~ states using Add Disk control 412 and Delete Disk control 414. The size of an image (if any) installed on a disk must match the size of the disk. If the size is changed, then the image value changes to “None.” If the user selects an image that doesn’t match the size of the disk, then the disk resizes accordingly.

**Please amend the specification at Page 42, line 26 through Page 43, line 5:**

Access values pertaining to traffic direction (to and from) may be done by specifying a node name or by specifying an IP value/mask ~~pair~~, pair 442, as indicated by radio buttons 445 in the case of a “To” value. Selecting the “By Name” radio button 445 indicates that the user wishes to choose an interface 446 that exists in the farm. Any interface 446 can be selected, but when the firewall configuration is submitted using OK button 448, that interface 446 must be then currently wired to a subnet. If one of the “special” interfaces 446 is selected (e.g., the “outside”, “inside”, and “dmz” interfaces that refer to eth0, eth1, and eth2,

respectively, of the firewall that is being configured), then the rule refers to all traffic that incident to that ~~interface~~. interface 446. If a node's interface is referenced inside a firewall's rule configuration, then that node cannot be removed. In contrast, if the "By IP & Mask" radio button 445 is selected, then the user may specify a valid IP address and net mask for the current access specification.

**Please amend the specification at Page 43, lines 6-15:**

FIG. 4C is a diagram of a load balancer configuration dialog that may be used to create or modify one or more parameter values pertaining to a load balancer. Configuring a load balancer node involves providing one or more configuration parameter values in fields of a configuration dialog window 450. Within Window 450, a Name field 452 receives a value of a name for the load balancer node. A Type ~~field 452~~ field 454 is a select box giving possible Load balancer types. This field is modifiable when the node is designable. A Policy field 456 receives a value indicating the type of load-balancing policy that the load balancer should apply. The balancing policy that will be applied to traffic to the virtual IP of this load balancer. This field is modifiable when the node is editable. Examples of load balancing policies include Round Robin, etc.

**Please amend the specification at Page 60, lines 1-5:**

Servlet 812 passes FEML text 810' from server 804 to client 802, which stores FEML text 810. A JavaScript XML Parser process 824 is applied to FEML text 810, resulting in creating and storing FEML object model 808. Client 802 carries out a Generate-Farm process 826 on

FEML object model 808, resulting in creating and storing JavaScript object model 806, which may be imported into and manipulated by the client editor.